Secrecy Gain: a Wiretap Lattice Code Design

Jean-Claude Belfiore

Department of Communications and Electronics
TELECOM ParisTech
Paris
France
Email: belfiore@telecom-paristech.fr

Frédérique Oggier

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore
Email: frederique@ntu.edu.sg

Abstract—We propose the notion of secrecy gain as a code design criterion for wiretap lattice codes to be used over an additive white Gaussian noise channel. Our analysis relies on the error probabilites of both the legitimate user and the eavesdropper. We focus on geometrical properties of lattices, described by their theta series, to characterize good wiretap codes.

I. INTRODUCTION

The wiretap channel was introduced by Wyner [10] as a discrete memoryless broadcast channel where the sender, Alice, transmits confidential messages to a legal receiver Bob, in the presence of an eavesdropper Eve. Wyner defined the perfect secrecy capacity as the maximum amount of information that Alice can send to Bob while insuring that Eve gets a negligeable amount of information. He also described a generic coding strategy known as coset coding. While coset coding has been used in many coding scenarios (for ex. [11], [8]), Wyner used it to encode both data and random bits to confuse the eavesdropper. A more precise coset coding technique, called wiretap II codes, was presented in [7], where Alice enjoys a noiseless channel while Eve has to deal with a channel with erasures. The question of determining the secrecy capacity of many classes of channels has been addressed extensively recently, yielding a plethora of information theoretical results on secrecy capacity.

There is a sharp contrast with the situation of wiretap code designs, where very little is known. The most exploited approach to get practical codes so far has been to use LDPC codes (for example [9] for binary erasure and symmetric channels, [5] for Gaussian channels). We also note that wiretap II codes have been extended to more general settings such as network coding in [3]. Finally, lattice codes for Gaussian channels have been considered from an information theoretical point of view in [4].

The problem that we address in this paper is to propose a design criterion for constructing explicit lattice codes (of possibly small length) to be used over additive white Gaussian noise channels. Assuming that Eve's channel is worse than the one of Alice, we analyse the probability of both users to make a correct decision, and exhibit geometrical lattice properties that maximize Alice's probability of making the right decision, while minimizing Eve's probability of decoding successfully. These properties are captured by the theta series of the lattice used for encoding, which in turn is used to define the notion of *secrecy gain* as a measure of secrecy brough by the lattice wiretap codes. Note that we do not consider a binary input as proposed in [5].

The paper is organized as follows. In Section II, we first describe a coset coding strategy suitable for lattices, namely using coset lattice codes. The corresponding decoding strategy is described in Section III. The chore results are given in Section IV: Bob's and Eve's probability of decoding coset lattice codes are computed, and we show that the behaviour of its theta series captures what makes a lattice good for being a wiretap code, motivating the introduction of the notion of secrecy gain.

II. WIRETAP LATTICE ENCODING

We consider a Gaussian wiretap channel, namely a broadcast channel where the source (Alice) sends a signal to a legitimate receiver (Bob), while an illegitimate eavesdropper (Eve) can listen to the transmission. It is modeled by

$$
\begin{aligned}
y &= x + v_b \\
z &= x + v_e,
\end{aligned}
$$

where x is the transmitted signal, v_b and v_e denote the Gaussian noise at Bob, respectively Eve's side, both with zero mean, and respective variance σ_b^2 and σ_e^2. We assume that Bob has a good SNR, but that $\sigma_b^2 = N_0 << N_1 = \sigma_e^2$, so that Eve has a poor SNR, in particular with respect to Bob.

Alice's encoder maps k information symbols $s_1, \ldots, s_k$ from $\mathcal{S} = \{0, 1\}$ to a codeword $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, and over a transmission of n symbols, we get

$$
\begin{aligned}
\mathbf{y} &= \mathbf{x} + \mathbf{v}_b \\
\mathbf{z} &= \mathbf{x} + \mathbf{v}_e.
\end{aligned} \tag{1}
$$

Alice uses lattice coding, that is the codeword $\mathbf{x} = (x_1, \ldots, x_n)$ is actually a lattice point. A lattice Λ is a discrete set of points in $\mathbb{R}^n$, which can be described in terms of its generator matrix M by ([6], [1])

$$
\Lambda = \{\mathbf{x} = \mathbf{u}M \mid \mathbf{u} \in \mathbb{Z}^m\},
$$

where

$$
M = \begin{pmatrix}
v_{11} & v_{12} & \ldots & v_{1n} \\
v_{21} & v_{22} & \ldots & v_{2n} \\
\ldots & & \ldots & \\
v_{m1} & v_{m2} & \ldots & v_{mn}
\end{pmatrix}
$$

and

$$
\begin{aligned}
\mathbf{v}_1 &= (v_{11}, v_{12}, \ldots, v_{1n}), \\
\mathbf{v}_2 &= (v_{21}, v_{22}, \ldots, v_{2n}), \\
&\cdots \\
\mathbf{v}_m &= (v_{m1}, v_{m2}, \ldots, v_{mn}),
\end{aligned}
$$

are a linearly independent set of vectors in $\mathbb{R}^n$ (so that $m \leq n$) which form a basis of the lattice.

Alice chooses a lattice Λ_b (we use the subscript b to refer to the intended legitimate receiver Bob) and then encodes her k bits of information into a point $\mathbf{x} \in \Lambda_b$:

$$
\mathbf{s} = (s_1, \ldots, s_k) \in \{0,1\}^k \mapsto \mathbf{x} = (x_1, \ldots, x_n) \in \Lambda_b.
$$

In a practical scenario, a finite subset of Λ_b must be chosen as a function of the available power at the receiver, though for the analysis, we will often consider the infinite lattice, which is simpler to understand since we do not need to take into account the boundary effect.

In order to get confusion at the eavesdropper, we use coset coding, as proposed in [10], [7]. The idea (which has been used ever since, whenever there is wiretap coding) is that instead of having a one-to-one correspondence between $\mathbf{s} \in \{0,1\}^k \leftrightarrow \mathbf{x} \in \Lambda_b$, the vector of information symbols is mapped to a set of codewords, namely a coset (that is, a set of points obtained by translation of a lattice), after which a random point to be actually transmitted is chosen randomly inside the coset. More precisely, we partition the lattice Λ_b into a union of disjoint cosets of the form

$$
\Lambda_e + \mathbf{c},
$$

with Λ_e a sublattice of Λ_b and $\mathbf{c}$ an n-dimensional vector not in Λ_e. We need 2^k cosets to be labelled by $\mathbf{s} \in \{0,1\}^k$:

$$
\Lambda_b = \cup_{j=1}^{2^k} (\Lambda_e + \mathbf{c}_j).
$$

Since every coset contains the same number of elements, we have that

$$
|\Lambda_b / \Lambda_e| = 2^k. \tag{2}
$$

Once the mapping

$$
\mathbf{s} \mapsto \Lambda_e + \mathbf{c}_{j(\mathbf{s})}
$$

is done, Alice randomly chooses a point $\mathbf{x} \in \Lambda_e + \mathbf{c}_{j(\mathbf{s})}$ and sends it over the wiretap channel. This is equivalent to choose a random vector $\mathbf{r} \in \Lambda_e$. The transmitted lattice point $\mathbf{x} \in \Lambda_b$ is finally of the form

$$
\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_e + \mathbf{c}. \tag{3}
$$

We have denoted the sublattice Λ_e, since it encodes the random bits that are there to increase Eve's confusion, and is then the lattice intended for Eve.

Example 1: Take $\Lambda_b = \mathbb{Z}^2$ in $\mathbb{R}^2$ and $\Lambda_e = 2\mathbb{Z}^2$, for which we have

$$
\begin{aligned}
\mathbb{Z}^2 &= \{(x,y), \ x, y \in \mathbb{Z}\} \\
&= 2\mathbb{Z}^2 \cup (2\mathbb{Z}^2 + (0,1)) \cup (2\mathbb{Z}^2 + (1,0)) \cup (2\mathbb{Z}^2 + (1,1)).
\end{aligned}
$$

The lattice $\mathbb{Z}^2$ is thus partioned into $2^k = 4$ cosets, allowing to transmit $k = 2$ bits of information. Alice can then label any of the above 4 cosets, say

$$
\begin{aligned}
00 &\mapsto 2\mathbb{Z}_2, & 01 &\mapsto (2\mathbb{Z}_2 + (0,1)), \\
10 &\mapsto (2\mathbb{Z}_2 + (1,0)), & 11 &\mapsto (2\mathbb{Z}_2 + (1,1)).
\end{aligned}
$$

To transmit the two bits 01, she then randomly picks a point in the coset $2\mathbb{Z}_2 + (0,1)$, say $\mathbf{x} = (2,3)$, that is

$$
\mathbf{x} = \mathbf{r} + \mathbf{c} = 2(1,1) + (0,1),
$$

and sends this point over the wiretap channel.

By using lattice coset encoding, we notice that two lattices play a role:

- the lattice Λ_b, that Alice uses to communicate reliably with Bob,
- the lattice Λ_e, which is a sublattice of Λ_b, that appears in the process of coset coding for encoding random bits.

Our goal is to study how the properties of these two lattices are related to the design of good wiretap codes.

III. Wiretap Lattice Decoding

After transmission over the Gaussian wiretap channel, Bob and Eve receive respectively (see (1) and (3))

$$
\begin{aligned}
\mathbf{y} &= \mathbf{x} + \mathbf{v}_b &= \mathbf{r} + \mathbf{c} + \mathbf{v}_b \\
\mathbf{z} &= \mathbf{x} + \mathbf{v}_e &= \mathbf{r} + \mathbf{c} + \mathbf{v}_e,
\end{aligned}
$$

where we recall that $\mathbf{r} \in \Lambda_e$ encodes the random bits, and $\mathbf{c}$ is the coset representative of minimum energy labelled by the information bits. Both Bob and Eve are interested in decoding the information bits, namely in finding the correct coset that was sent. To do so, they need to find the closest lattice point in Λ_b to their respective received signal $\mathbf{y}$ or $\mathbf{z}$, from which they deduce the coset to which it corresponds.

Recall that for any lattice point P_i of a lattice $\Lambda \subset \mathbb{R}^n$, its Voronoi cell is defined by

$$
\mathcal{V}(P_i) = \{\mathbf{x} \in \mathbb{R}^n, \ d(\mathbf{x}, P_i) \leq d(\mathbf{x}, P_j) \text{ for all } j\}.
$$

Since all lattice points have the same Voronoi cell, we will speak of the Voronoi cell of the lattice Λ and denote it by $\mathcal{V}(\Lambda)$.

Now when transmitting a codeword $\mathbf{x}_k$ in $\mathbb{R}^n$ with Voronoi cell $\mathcal{V}(\mathbf{x}_k)$ over an additive white Gaussian noise channel with noise variance σ^2, the decoder makes the correct decision if and only if the noise vector is in $\mathcal{V}(\mathbf{x}_k)$, an event of probability

$$
\frac{1}{(\sigma\sqrt{2\pi})^n} \int_{\mathcal{V}(\mathbf{x}_k)} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u}.
$$

In our scenario, the probability P_c of correct decision concerns not just one point but a coset, and thus it is the probability that the received signal lies in the union of the Voronoi regions of Λ_b, translated by points of Λ_e. Suppose that the lattice point $\mathbf{x}_k = \mathbf{r}_k + \mathbf{c}_k \in \Lambda_b$ has been transmitted. The probability P_c of finding the correct coset is thus, assuming no boundary effect

$$
P_c = \frac{1}{(\sigma\sqrt{2\pi})^n} \sum_{\mathbf{r} \in \Lambda_e} \int_{\mathcal{V}(\mathbf{x}_k)+\mathbf{r}} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u}.
$$

If we take M codewords $\mathbf{x}_1, \ldots, \mathbf{x}_M$ from Λ_b, then as already noticed, all Voronoi cells are the same, namely $\mathcal{V}(\mathbf{x}_k) = \mathcal{V}(\Lambda)$, $k = 1, \ldots, M$, and thus we get

$$P_c = \frac{1}{(\sigma\sqrt{2\pi})^n} \sum_{\mathbf{r}\in\Lambda_e} \int_{\mathcal{V}(\Lambda_b)+\mathbf{r}} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u}. \qquad (4)$$

IV. WIRETAP LATTICE CODE DESIGN

We now study the probability of Bob and Eve to make a correct decoding decision, and try to maximize Bob's probability while minimizing the one of Eve. This leads us to study the theta series of the lattices involved.

A. A first analysis

Considering the wiretap channel (1) where Alice transmits lattice codewords from an n-dimensional lattice Λ_b, we thus get from (4) that the probability $P_{c,b}$ of Bob's (resp. $P_{c,e}$ of Eve's) correct decision is:

$$\begin{aligned}
P_{c,b} &= \frac{1}{(\sqrt{2\pi}\sigma_b)^n} \sum_{\mathbf{r}\in\Lambda_e} \int_{\mathcal{V}(\Lambda_b)+\mathbf{r}} e^{-||\mathbf{u}||^2/2\sigma_b^2} d\mathbf{u} \\
P_{c,e} &= \frac{1}{(\sqrt{2\pi}\sigma_e)^n} \sum_{\mathbf{r}\in\Lambda_e} \int_{\mathcal{V}(\Lambda_b)+\mathbf{r}} e^{-||\mathbf{u}||^2/2\sigma_e^2} d\mathbf{u}.
\end{aligned}$$

Since by assumption Bob has a good SNR, its received vector $\mathbf{y}$ is most likely to lie in the Voronoi region around the origin, and thus the terms corresponding to $\mathbf{r} \neq \mathbf{0}$ in (4) are negligeable, which yields:

$$P_{c,b} \simeq \frac{1}{(\sqrt{2\pi}\sigma_b)^n} \int_{\mathcal{V}(\Lambda_b)} e^{-||\mathbf{u}||^2/2\sigma_b^2} d\mathbf{u}. \qquad (5)$$

This is now the familiar case of transmitting lattice points over the Gaussian channel, for which it is known that Λ_b should have a good Hermite parameter, to get a good coding gain.

We are on the contrary under a low SNR assumption for Eve, namely σ_e is large, and thus a Taylor expansion at order 0 gives

$$e^{-||\mathbf{w}+\mathbf{r}||^2/2\sigma^2} = e^{-||\mathbf{r}||^2/2\sigma^2} + O\left(\frac{1}{\sigma_e^2}\right)$$

so that

$$\begin{aligned}
\int_{\mathcal{V}(\Lambda_b)+\mathbf{r}} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u} &= \int_{\mathcal{V}(\Lambda_b)} e^{-||\mathbf{w}+\mathbf{r}||^2/2\sigma^2} d\mathbf{w} \\
&\simeq \mathrm{Vol}(\mathcal{V}(\Lambda_b)) e^{-||\mathbf{r}||^2/2\sigma^2},
\end{aligned}$$

where the volume $\mathcal{V}(\Lambda_b)$ of the lattice is

$$\mathrm{Vol}(\mathcal{V}(\Lambda)) = \int_{\mathcal{V}(\Lambda)} d\mathbf{x} = \det(MM^T)^{1/2}.$$

The probability of making a correct decision for Eve is then

$$P_{c,e} \simeq \frac{1}{(\sqrt{2\pi}\sigma_e)^n} \mathrm{Vol}(\mathcal{V}(\Lambda_b)) \sum_{\mathbf{r}\in\Lambda_e} e^{-||\mathbf{r}||^2/2\sigma_e^2}, \qquad (6)$$

from which we get that

$$\frac{P_{c,e}}{P_{c,b}} \simeq \left(\frac{\sigma_b}{\sigma_e}\right)^n \mathrm{Vol}(\mathcal{V}(\Lambda_b)) \frac{\sum_{\mathbf{r}\in\Lambda_e} e^{-||\mathbf{r}||^2/2\sigma_e^2}}{\int_{\mathcal{V}(\Lambda_b)} e^{-||\mathbf{u}||^2/2\sigma_b^2} d\mathbf{u}} \qquad (7)$$

We know how to design good codes for Bob's channel, and have his probability of making a correct decision arbitrarily close to 1. Our aim is thus to minimize the probability $P_{c,e}$ of Eve making a correct decision, while keeping $P_{c,b}$ unchanged. This is equivalent to minimize (7), that is to find a lattice Λ_b which is as good as possible for the Gaussian channel [1], and

$$\boxed{\begin{array}{c} \text{minimize } \sum_{\mathbf{r}\in\Lambda_e} e^{-||\mathbf{r}||^2/2\sigma_e^2} \\ \text{under the constraint } \log_2 |\Lambda_b/\Lambda_e| = k. \end{array}} \qquad (8)$$

The constraint on the cardinality of cosets (or rate) is equivalent to set the fundamental volume of Λ_e equal to a constant.

It is natural to start by approximating the sum of exponentials by its terms of higher order, namely

$$\begin{aligned}
\sum_{\mathbf{r}\in\Lambda_e} e^{-||\mathbf{r}||^2/2\sigma_e^2} &\simeq 1 + \sum_{\mathbf{r}\in\Lambda_e, ||\mathbf{r}||=d_{\min}(\Lambda_e)} e^{-||\mathbf{r}||^2/2\sigma_e^2} \\
&= 1 + \tau(\Lambda_e) e^{-d_{\min}(\Lambda_e)^2/2\sigma_e^2},
\end{aligned}$$

where $\tau(\Lambda_e)$ is the kissing number of Λ_e which counts the number of vectors of length $d_{\min}(\Lambda_e)$. Thus as a first criterion, we should maximize $d_{\min}(\Lambda_e)$ while preserving the fundamental volume of Λ_e, which is equivalent to require for Λ_e to have a good Hermite parameter

$$\gamma_H(\Lambda) = \frac{d_{\min}^2(\Lambda)}{\det(MM^T)^{1/n}}.$$

after which we should minimize its kissing number. This approximation however assumes high SNR, which typically Eve does not have. We thus cannot be content with this approximation, and have to obtain a more precise analysis.

B. The secrecy gain

Let us get back to the code design criterion (8) and rewrite it in terms of the theta serie of the lattice considered.

Recall that given a lattice $\Lambda \subset \mathbb{R}^n$, its *theta serie* Θ_Λ is defined by ([1])

$$\Theta_\Lambda(z) = \sum_{\mathbf{x}\in\Lambda} q^{||\mathbf{x}||^2}, \; q = e^{i\pi z}, \mathrm{Im}(z) > 0. \qquad (9)$$

Exceptional lattices have theta series that can be expressed as functions of the Jacobi theta functions $\vartheta_i(q)$, $i = 2, 3, 4$, themselves defined by

$$\vartheta_2(q) = \sum_{n=-\infty}^{+\infty} q^{\left(n+\frac{1}{2}\right)^2},$$

$$\vartheta_3(q) = \sum_{n=-\infty}^{+\infty} q^{n^2},$$

$$\vartheta_4(q) = \sum_{n=-\infty}^{+\infty} (-1)^n q^{n^2}.$$

Example 2: Here are a few examples of theta series for some exceptional lattices.

1) The cubic lattice $\mathbb{Z}^n$:

$$\Theta_{\mathbb{Z}^n}(q) = \vartheta_3(q)^n.$$

2) D_n:
$$\Theta_\Lambda(D_n) = \frac{1}{2} \left(\vartheta_3(q)^n + \vartheta_4(q)^n \right).$$

3) The Gosset lattice E_8:
$$\Theta_{E_8}(q) = \frac{1}{2} \left(\vartheta_2(q)^8 + \vartheta_3(q)^8 + \vartheta_4(q)^8 \right).$$

4) The Leech lattice Λ_{24}:
$$\Theta_{\Lambda_{24}}(q) = \frac{1}{8} \left(\vartheta_2(q)^8 + \vartheta_3(q)^8 + \vartheta_4(q)^8 \right)^3$$
$$- \frac{45}{16} \vartheta_2(q)^8 \vartheta_3(q)^8 \vartheta_4(q)^8.$$

From (8), we need to minimize
$$\sum_{\mathbf{r} \in \Lambda_e} e^{-\|\mathbf{r}\|^2 / 2\sigma_e^2} = \sum_{\mathbf{r} \in \Lambda_e} \left(e^{-1/2\sigma_e^2} \right)^{\|\mathbf{r}\|^2}$$
$$= \sum_{\mathbf{r} \in \Lambda_e} \left((e^{i\pi})^{-1/2i\pi\sigma_e^2} \right)^{\|\mathbf{r}\|^2}$$
$$= \Theta_{\Lambda_e} \left(z = \frac{-1}{2i\pi\sigma_e^2} \right)$$

with $q = e^{i\pi z}$ and
$$\mathrm{Im} \left(\frac{-1}{2i\pi\sigma_e^2} \right) = \mathrm{Im} \left(\frac{i}{2\pi\sigma_e^2} \right) > 0.$$

Thus to minimize Eve's probability of correct decision is equivalent to minimize $\Theta_{\Lambda_e}(z)$ in $z = i/2\pi\sigma_e^2$. To approach this problem, let us set $y = -iz$ and restrict to real positive values of y. We are now interested in minimizing
$$\Theta_{\Lambda_e}(y) = \sum_{\mathbf{r} \in \Lambda_e} q^{\|\mathbf{r}\|^2}, \quad q = e^{-\pi y}, y > 0,$$

in the particular value of y corresponding to $z = i/2\pi\sigma_e^2$, namely
$$y = \frac{1}{2\pi\sigma_e^2}.$$

This is actually a problem that classically arises in the study of theta series [2]: given the lattice dimension n, find the lattice $\Lambda^\star$ that minimizes $\Theta_\Lambda(y)$ for a given value of y.

Note that if Λ_e is not chosen to be a particular lattice, we can assume that $\Lambda_e = \mathbb{Z}^n$. We consequently define the secrecy function of a given lattice Λ as the ratio of its theta series and the theta series of $\mathbb{Z}^n$, in a chosen point y.

Definition 1: Let Λ be an $n-$dimensional lattice. The *secrecy function* of Λ is given by
$$\Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \frac{\vartheta_3(y)^n}{\Theta_\Lambda(y)}$$

defined for $y > 0$.

As we want to minimize the expression of Eve's probability of correct decision in (8), we are interested in the maximum value of the secrecy function. This yields the notion of secrecy gain.

Definition 2: The *secrecy gain* χ_Λ of an $n-$dimensional lattice Λ is defined by
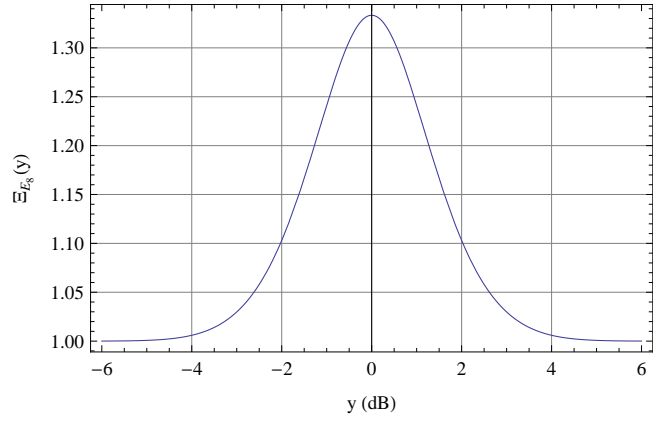$$\chi_\Lambda = \sup_{y > 0} \Xi_\Lambda(y).$$
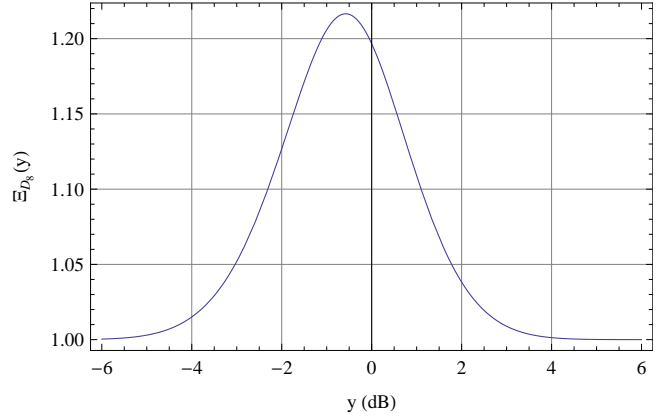

Fig. 1. Secrecy function of E_8.

Fig. 2. Secrecy function of D_8.

Examples of the secrecy function for the lattices E_8 and D_8 are shown in Figures 1 and 2, respectively. Both lattices clearly have a maximum, happening in $y = 1$ for E_8 but not for D_8 (which is conjectured to have this maximum in $\frac{1}{\sqrt[4]{2}}$).

It is worth emphasizing that the value at which the secrecy function gets its maximum is important for the code design, since it tells us what is the SNR at which the wiretap lattice code is providing most confusion to Eve. The two examples suggest that this value depends on the chosen lattice.

Conjectures on the behaviour of the secrecy gain are currently being investigated. It is expected that an asymptotic analysis will give a first insight, and that a finer study should reveal how the secrecy gain is connected to the equivocation rate.

Let us conclude by giving a small example of code construction.

Example 3: Consider the case of an $8-$dimensional (real) construction. Suppose we want to transmit at a secrecy rate of 2 bits per complex symbol. We choose $\Lambda_b = E_8$, since this lattice has the best coding gain and the best shaping gain in dimension 8. For Λ_e, we choose as sublattice of E_8 the lattice $2E_8$, a scaled version of Λ_b. We then have
$$|E_8/2E_8| = 256$$

which gives as rate per complex symbol

$$R = \frac{1}{4} \log_2 |E_8/2E_8| = 2$$

which is the requested rate.

To construct E_8 while preserving the overall shaping, we choose a construction A [1]:

$$E_8 = 2\mathbb{Z}^8 + (8, 4, 4)$$

where $(8, 4, 4)$ stands for the Reed-Müller code of length 8 and dimension 4. We repeat the same construction for $2E_8$, namely

$$2E_8 = 4\mathbb{Z}^8 + 2 \cdot (8, 4, 4).$$

We can now give a construction of E_8 using $2E_8$:

$$E_8 = 2E_8 + (8, 4, 4) + 2 \cdot \mathcal{C}_\dagger$$

where $\mathcal{C}_\dagger$ is the set of all representatives of the cosets of $(8, 4, 4)$ with minimum Hamming weights. This yields

$$E_8/2E_8 = (8, 4, 4) + 2 \cdot \mathcal{C}_\dagger$$

which gives an alphabet with 256 codewords.

Then, the random bits label $2E_8$, which means that 4 of these bits serve as information bits for $2 \cdot (8, 4, 4)$ and the other ones label points of $4\mathbb{Z}^8$.

It has been proved [2], and this is the best result known up to date, that some lattices, including E_8, reach a local minimum of their theta series for some constant $y > 0$ close to 1. Thus using $\Lambda_e = 2E_8$ indeed helps in optimizing the secrecy gain.

V. CURRENT AND FUTURE WORK

In this paper, we provided a practical wiretap coding scheme using coset lattice codes. We exhibited geometric properties that a lattice and its sublattice should satisfy to provide good wiretap codes for transmission over additive white Gaussian noise channels, in terms of the theta series of the involved lattices. This yielded the notion of secrecy gain. Our analysis focuses on error probabilities of both users rather than on equivocation rate, though we expect that further work will enlighten the connection between the two concepts.

We are currently studying different conjectures on the behaviour of the secrecy gain, as well as the design of lattice codes that fullfil the code design criteria. Having explicit constructions of families of wiretap codes to compare will give us a further understanding of what is a good wiretap lattice code. It is also a natural work to address the achievability of such codes with respect to the secrecy capacity of Gaussian channels.

Finally, lattice codes have also been useful to design modulation schemes for fading channels. It is a natural generalization to consider a similar analysis of what makes a good wiretap code in the context of fading channels.

REFERENCES

[1] J.H. Conway, N.J.A. Sloane, "Sphere packings, Lattices and Groups," Third edition, *Springer-Verlag*, New York, 1998.
[2] R. Coulangeon, "Spherical designs and zeta functions of lattices," *http://arxiv.org/abs/math/0611735*.
[3] S. Y. El Rouayheb, E. Soljanin, "On Wiretap Networks II," *Proc. ISIT*, 2007.
[4] Xiang He and Aylin Yener, "Providing Secrecy With Structured Codes: Tools and Applications to Two-User Gaussian Channels," preprint, arxiv.org/pdf/0907.5388.
[5] D.Klinc, J.Ha, S.W.McLaughlin, J.Barros, and B.J.Kwak, "LDPC Codes for the Gaussian Wiretap Channel," *Proc. Information Theory Workshop (ITW)*, Oct. 2009.
[6] F. Oggier, E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," *Foundations and Trends in Communications and Information Theory*, December 2004.
[7] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. Journal*, vol. 63, no. 10, pp. 2135-2157, Dec. 1984.
[8] S.S. Pradhan, K. Ramchandran, "Generalized Coset Codes for Distributed Binning", *IEEE Transactions on Information Theory*, OCtober 2005.
[9] A. Thangaraj, S. Dihidar, A. R. Calderbank, S.W. McLaughlin, and J.-M. Merolla, "Applications of LDPC Codes to the Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 53, No. 8, Aug. 2007
[10] A.D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, October 1975.
[11] R. Zamir, S. Shamai, U. Erez, "Linear/Lattice Codes for Structured Multi-terminal Binning", *IEEE Transactions on Information Theory*, June 2002.